

## **REMARKS**

Claims 1 – 17 are currently pending.

Claims 1 – 17 were rejected pursuant to 35 U.S.C. § 103(a) as being unpatentable over Affleck et al. (U.S. Publication No. 2004/0260782) in view of Thompson (U.S. Publication No. 2005/0055709). Applicant respectfully request reconsideration of the claim rejections in view of the claim amendments and the following remarks.

### **I. Claim Rejections – 35 U.S.C. § 103(a)**

Claims 1 – 8 were rejected pursuant to 35 U.S.C. § 103(a) as being unpatentable over Affleck et al. in view of Thompson.

Amended claims 1 and 5 recite enabling access authorization to the system technician when the first authentication is authenticated at the first data processing unit and the second authentication is authenticated at the second data processing unit.

Affleck et al. relates to a “user interface [that] comprises a setup module 405, an image module 430, a schedule manager 450, a plate handler 420, an environment monitoring and control module 470, and a result analyzer 460” (paragraph [0062]). The setup module 405 may include a system administration module 410 (paragraph [0065]). The system administration module 410 comprises a security module 550 (paragraph [0065]). Affleck et al. describes the security module 550 as follows:

The security module 550 allows the system administrator to edit access rights of each of the technicians. Access rights for individual technicians, or groups of technicians, may be set or edited, and logon attempts may be monitored. In order for the technician to gain access to the user interface 150, the technician must first be authenticated, by entering a login name and password, for example. See, Affleck et al., paragraph [0066], emphasis added.

Thompson relates to:

A cable distribution box, including an authentication device obtaining authentication information from an authentication medium, an access administration system operatively connected to the authentication device for verifying the authentication information and collecting work log data, and an access control system operatively connected to the access administration system granting access to the cable distribution box when the authentication information is verified. See, Thompson, Abstract

Neither Affleck et al. or Thompson, alone or in combination, disclose “enabling access authorization to the system technician when the first authentication is authenticated at the first data processing unit and the second authentication is authenticated at the second data processing unit,” as claimed in claims 1 and 5. Affleck et al. discloses a security module 550 that may be used to restrict access to a technician (paragraph [0066]). The system administrator may use the security module 550 to restrict a technician from gaining access to the user interface, for example, by deleting the technicians’ name (paragraph [0066]). In other words, Affleck et al. enables authentication to the system technician when the technicians’ authentication is authenticated. However, Affleck et al. is completely silent as to enabling access authorization to the technician when the technicians’ authentication is authenticated and the system administrators authentication is authenticated.

Thompson also fails to disclose this feature. Thompson discloses an access administration system that verifies information. Thompson is completely silent as to enabling access authorization to a system technician when a first authentication is authenticated at the first data processing unit and the second authentication is authenticated at the second data processing unit.

Accordingly, since neither Affleck et al. nor Thompson, alone or in combination, disclose the claimed feature, claims 1 and 5 are allowable over the cited references.

Dependent claims 2 – 4 and 6 – 8 depend from allowable claim 1 and are allowable for at least these reasons. Further limitations of the dependent claims are allowable over the cited references.

Claims 6, 7, and 8 recite that the authentication code is stored in a mobile memory unit that can be connected to the data processing system to transmit data. The Office Action cites Thompson as disclosing this feature (Office Action, page 6). However, the cited portion of Thompson does not disclose an authentication card, as stated in the Office Action. The cited portion of Thompson discloses readers; not cards. Accordingly, Thompson is completely silent as to that the authentication code is stored in a mobile memory unit that can be connected to the data processing system to transmit data. Therefore, claims 6, 7, and 8 are allowable over the cited references.

Claims 9 – 17 were rejected pursuant to 35 U.S.C. § 103(a) as being unpatentable over Affleck et al. in view of Thompson.

Amended claim 9 recites checking whether the first authentication and second authentication are authenticated at the same time; and enabling access authorization to the system technician when the first authentication and second authentication are authenticated at the same time.

Affleck et al. is discussed above.

Thompson is discussed above.

Neither Affleck et al. nor Thompson, alone or in combination, disclose “checking whether the first authentication and second authentication are authenticated at the same time; and enabling access authorization to the system technician when the first authentication and second authentication are authenticated at the same time,” as claimed in claim 9. As discussed above, Affleck et al. is directed to checking whether the technicians authentication is authenticated. Thompson is directed to an access administration system that verifies information

for a single cable distribution box 308 (See, e.g., paragraphs [0028] – [0031]. Thompson does not disclose checking whether the first authentication and second authentication are authenticated at the same time. Therefore, claim 9 is allowable over the cited references.

Dependent claims 10 – 17 depend from allowable claim 9 and are allowable for at least these reasons. As discussed below, further limitations of the dependent claims may be allowable over the cited references.

Claim 10 recites that the data processing system processes data that can be accessed by by individuals with a simple authorization according to the two man principle when the particular authorization is not present. The cited references fail to disclose the two man principle. The two man principle may be defined as follows:

**two-person integrity** A security practice designed to prevent an individual from having solitary access to sensitive data, equipment or other material. Two-person integrity requires at least two authorized individuals to be involved in the performance of a task, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. One person performs the task and the other keeps a watchful eye on it being performed. See, Newton's Telecom Dictionary, Copyright © Harry Newton, 24<sup>th</sup> Edition

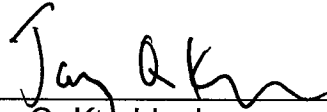
One skilled in the art would understand that the cited portion of Affleck et al. does not disclose the two-man principle. Therefore, claim 10 is allowable over the cited references.

**Conclusion**

For at least the reasons presented above, the Applicant respectfully submits that the pending claims are in condition for allowance.

The Examiner is respectfully requested to contact the undersigned in the event that a telephone interview would expedite consideration of the application.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Jay Q. Knobloch", written over a horizontal line.

Jay Q. Knobloch  
Registration No. 57,347  
Attorney for Applicant

BRINKS HOFER GILSON & LIONE  
P.O. BOX 10395  
CHICAGO, ILLINOIS 60610  
(312) 321-4200